UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,117	06/30/2000	Kelan C. Silvester	042390.P8691	1041

7590 12/21/2004

Walter T Kim
Blakely Sokoloff Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/608,117	SILVESTER, KELAN C.	
	Examin r	Art Unit	
	Brandon Hoffman	2136	

-- Th MAILING DATE of this communication appears on the cov r sh et with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-19,21 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-19,21 and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-5, 7-19, 21, and 22 are pending in this office action.

2. Applicant's arguments filed August 30, 2004, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Claim Rejections - 35 USC § 103

4. Claims 1-5, 7-19, 21, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones et al. (U.S. Patent No. 5,623,637) in view of Cripe et al. (U.S. Patent No. 5,754,821).

Regarding claim 1, Jones et al. teaches a method comprising:

- Providing a partition on a storage device of a computer system (col. 5, lines 32-34);
- Providing a software task having knowledge about a proper handshake to unlock the partition such that the partition that was previously invisible to the operating system becomes visible to the operating system (col. 8, lines 4-34, the particular

method of combining passwords, random numbers, and an unlock code has to be known by the software task in order for the unlocking to be performed properly); and

- Unlocking the partition in response to an unlock request received from the software task having knowledge about the handshake to unlock the partition (col. 5, lines 59-67).

Jones et al. does not teach wherein said partition is invisible to an operating system of the computer system unless the partition is unlocked or wherein the partition is visible to the operating system when unlocked.

Cripe et al. teaches wherein said partition is invisible to an operating system of the computer system unless the partition is unlocked and wherein the partition is visible to the operating system when unlocked (col. 2, lines 8-24).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine wherein said partition is invisible to an operating system of the computer system unless the partition is unlocked or wherein the partition is visible to the operating system when unlocked, as taught by Cripe et al., with the method of Jones et al. It would have been obvious for such modifications because this prevents the secured partition from exchanging information with the host (see col. 4, lines 47-50 of Jones et al.).

Regarding claim 2, Jones et al. as modified by Cripe et al. teaches wherein the storage device is a hard disk drive having a disk controller (see fig. 1, ref. num 40 of Cripe et al.).

Regarding claim 3, Jones et al. as modified by Cripe et al. teaches wherein the unlocking of the partition is initiated by establishing a proper unlock handshake between the software task and an IDE controller for controlling the storage device (see col. 8, lines 9-34, col. 3, lines 64-67, & fig. 2 of Jones et al.).

Regarding claim 4, Jones et al. as modified by Cripe et al. teaches wherein the software task requests a master token from the IDE controller when the computer system is first turned on and the unlock handshake between the software task and the IDE controller is established by passing the master token back to the IDE controller as a parameter (see col. 7, lines 52-58 and col. 8, lines 9-34 of Jones et al.).

Regarding claim 5, Jones et al. as modified by Cripe et al. teaches wherein the software task requests a master token from the disk controller when the computer system is first turned on (see col. 7, lines 52-58 of Jones et al.), said master token is used by the software task to initiate the proper handshake to unlock the partition (see col. 8, lines 4-34 of Jones et al.).

Regarding claim 7, Jones et al. as modified by Cripe et al. teaches wherein the software receives a usage token from an IDE controller when the partition is unlocked and the access handshake between the software and the IDE controller is established by passing the usage token back to the IDE controller as a parameter (the Examiner takes Official Notice that this action is required in public-key cryptography. IDE controller sends a public key to the software, the software encrypts its request with the public key of the IDE controller, and the IDE controller decrypts the request with its private key).

Regarding claim 8, Jones et al. as modified by Cripe et al. teaches further comprising locking the partition in response to a lock request received from a software having knowledge about a proper handshake for locking the partition (see col. 7, lines 21-31 of Jones et al.).

Regarding claim 9, Jones et al. as modified by Cripe et al. teaches further comprising providing a standard partition on the storage device (see col. 7, lines 32-35 of Jones et al.), wherein said standard partition is always visible to the operating system and generally accessible to other software (see col. 7, lines 32-35 of Jones et al.).

Regarding claim 10, Jones et al. teaches a machine-readable medium that provides instructions, which when executed by a set of processors, causes said set of processors to perform operations comprising:

- Receiving an open request from a software to access a secure-private partition on a hard drive of a computer system (col. 5, lines 54-59);
- Validating the open request received from the software (col. 5, lines 59-64);
- Requesting unlocking of the secure-private partition in response to the validation of the open request received from the software (col. 5, lines 64-67);
- Unlocking the secure-private partition in response to the unlocking request (col. 5, lines 59-67 and col. 6, lines 1-4); and
- Preventing an access to the secure-private partition when the secure-private partition is unlocked unless the access is requested by a software having knowledge about a proper access handshake for accessing the secure-private partition (col. 8, lines 4-34, the particular method of combining passwords, random numbers, and an unlock code has to be known by the requesting software in order for the unlocking to be performed properly).

Jones et al. does not teach such that the partition that was previously invisible to an operating system becomes visible to the operating system.

Cripe et al. teaches such that the partition that was previously invisible to an operating system becomes visible to the operating system (col. 2, lines 8-24).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine such that the partition that was previously invisible to

an operating system becomes visible to the operating system, as taught by Cripe et al. with the medium of Jones et al. It would have been obvious for such modifications because this prevents the secured partition from exchanging information with the host (see col. 4, lines 47-50 of Jones et al.).

Regarding claim 11, Jones et al. as modified by Cripe et al. teaches wherein the operations further comprise requesting locking of the secure-private partition in response to a close request received from the software (see col. 7, lines 21-31 of Jones et al.).

Regarding claim 12, Jones et al. as modified by Cripe et al. teaches wherein the requesting of the unlocking of the secure partition further comprises:

- Requesting a master token from an IDE controller when the computer system is turned on (see col. 7, lines 52-58 of Jones et al.);
- Storing the master token in a secure storage location (see col. 8, lines 6-9 of Jones et al.);
- Retrieving the master token from the secure storage location when an access to a secure-private partition is needed (see col. 8, lines 9-34 of Jones et al.); and
- Passing the master token as a parameter to the IDE controller (see col. 8, lines 20-24 of Jones et al.).

Regarding claim 13, Jones et al. as modified by Cripe et al. teaches wherein the operations further comprise requesting an access to the secure-private partition in response to an access request received from the software (see col. 6, lines 1-4 of Jones et al.).

Regarding claim 14, Jones et al. as modified by Cripe et al. teaches wherein the requesting of the access to the secure partition further comprises:

- Receiving a usage token (see fig. 2, ref. num 303 and col. 8, lines 9-13 of Jones et al.); and
- Passing the usage token to the IDE controller to gain an access to the secure partition (see fig. 2, ref. num 307 and col. 8, lines 9-19 of Jones et al.).

Regarding claim 15, Jones et al. as modified by Cripe et al. teaches wherein the request from the software to access the secure-private partition is received by a privacy gatekeeper which prescreens the request to determine if the software has an authorization to access the secure-private partition (see col. 7, lines 52-59 of Jones et al., describes authorizing the request as soon as the card is inserted, or at first turning on the computer. This is the prescreening, if the authorization fails, the computer system knows the device is not authorized for future transactions, and vice versa.).

Regarding claim 16, Jones et al. teaches a system comprising:

- A storage device having a storage controller (fig. 1, ref. num 100),

- Said storage device having at least one secure-private partition (fig. 1, ref. num 150),
- Wherein said secure-private partition is selectively in one of locked and unlocked modes (col. 7, lines 21 and 36);

- An IDE controller operatively coupled to the storage controller (col. 3, lines 64-67); and
- A security/privacy software task operatively coupled to the IDE controller (fig. 1, ref. num 220),
  - Wherein said IDE controller initiates an unlock request to unlock the secure-private partition in response to a valid unlock handshake established between the IDE controller and the security/privacy software task (col. 5, lines 59-67) and
  - Said IDE controller initiates a lock request to lock the secure-private partition in response to a valid lock handshake established between the IDE controller and the security/privacy software task (col. 7, lines 21-31).

Jones et al. does not teach wherein said secure-private partition is invisible to an operating system when it is locked and the secure-private partition is visible to the operating system when it is unlocked.

Cripe et al. teaches wherein said secure-private partition is invisible to an operating system when it is locked and the secure-private partition is visible to the operating system when it is unlocked (col. 2, lines 8-24).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine wherein said secure-private partition is invisible to an operating system when it is locked and the secure-private partition is visible to the operating system when it is unlocked, as taught by Cripe et al., with the system of Jones et al. It would have been obvious for such modifications because this prevents the secured partition from exchanging information with the host (see col. 4, lines 47-50 of Jones et al.) and the interface provides a way to exchange control signals from the secure storage are to the host computer.

Regarding claim 17, Jones et al. as modified by Cripe et al. teaches wherein the security/privacy software task requests a master token from the IDE controller when the system is turned on and sends the master token to the IDE controller as a parameter when making a request to the IDE controller to unlock the secure-private partition (see col. 7, lines 52-58 and col. 8, lines 9-34 of Jones et al.).

Regarding claim 18, Jones et al. as modified by Cripe et al. teaches further comprising a requesting software and a privacy gatekeeper which acts as a gatekeeper to the security/privacy software task (see fig. 1, ref. num 178 of Jones et al.), wherein

when the requesting software makes a request to access the secure-private partition (see col. 5, lines 59-67 of Jones et al.), the privacy gatekeeper prescreens the request to determine if the requesting software has an authorization to access the secure-private partition (see col. 7, lines 52-59 of Jones et al., describes authorizing the request as soon as the card is inserted, or at first turning on the computer.).

Regarding claim 19, Jones et al. as modified by Cripe et al. teaches wherein the IDE controller allows an access to said at least one secure-private partition only when a valid access handshake is established between the requesting software and the IDE controller (see col. 8, lines 9-34 & fig. 2 of Jones et al.).

Regarding claim 21, Jones et al. as modified by Cripe et al. teaches preventing an access to the partition when the partition is unlocked unless the access is requested by a software having knowledge about a proper access handshake for accessing the partition (see col. 8, lines 4-34 of Jones et al., the particular method of combining passwords, random numbers, and an unlock code has to be known by the requesting software in order for the unlocking to be performed properly).

Regarding claim 22, Jones et al. as modified by Cripe et al. teaches wherein the DE controller generates and return a usage token to the requesting software once the secure-private partition is unlocked, wherein the access handshake is established between the IDE controller and the requesting software when the IDE controller

validates the usage token passed back by the requesting software (see col. 8, lines 4-34 of Jones et al., the particular method of combining passwords, random numbers, and an unlock code has to be known by the requesting software in order for the unlocking to be performed properly).

Response to Arguments

5. Applicant argues:

a. The independent claims are not shown to "provide an invisible partition unless the partition is locked," but rather show that the partition is inaccessible, not invisible (page 6, third paragraph, page 7, last paragraph, and page 8, last paragraph).

b. The dependent claims are allowable based on their dependency on the independent claims (page 7, third paragraph, page 8, third paragraph, and page 9, last paragraph).

Regarding argument (a), examiner disagrees with applicant. The "fence" in Cripe et al. is used to protect the system partition from access at the operating system level (see col. 1, lines 62-66). The fence is 'set' by providing an undocumented command that changes the total address size of the DASD (direct access storage device) to be the total address size of the DASD minus the size of the protected system partition (see col. 2, lines 8-17). The remainder of the paragraph (see col. 2, lines 17-24) shows that by the time the operating system load is started, the system partition is hidden/invisible

to the operating system. The remainder of Cripe et al. shows how to gain access to the protected (invisible) system partition (see col. 2, line 65 through col. 3, line 32).

Regarding argument (b), examiner disagrees with applicant. Based on the arguments set forth by the examiner for argument (a), the dependent claims stand as rejected.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brenda Hoff

BH

EMMANUEL L. MOISE
PRIMARY EXAMINER